MICHAEL SULLIVAN
UNITED STATES ATTORNEY
DISTRICT OF MASSACHUSETTS
PREPARED REMARKS FOR THE
SUBCOMMITTEE ON CRIME, TERRORISM , AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES
MAY 3, 2005

I. Introduction

Mr. Chairman, Ranking Member Scott, and Members of the Subcommittee, thank you for the invitation to appear before you today to discuss several important provisions of the USA PATRIOT Act. I will address sections 201 and 202 of the Act, which provide law enforcement with the ability to use pre-existing wiretap authorities to investigate certain crimes that terrorists are likely to commit, such as those involving weapons of mass destruction, material support to terrorists and foreign terrorist organizations, and important cybercrime and cyberterrorism offenses. I also will address section 223, which allows an individual whose privacy is violated to sue the United States for money damages if its officers or employees disclose sensitive information without authorization. All three of these sections are currently scheduled to sunset at the end of 2005. If sections 201 and 202 are allowed to sunset, we will lose valuable tools that allow law enforcement to investigate a full range of terrorism-related crimes. Paradoxically, these tools would be unavailable in criminal terrorism investigations of offenses involving chemical weapons, cyberterrorism, or weapons of mass destruction, but would be available to investigate traditional crimes such as drug offenses, mail fraud, and passport fraud. This would be a senseless approach. Because it is absolutely vital that the Justice Department have all appropriate tools at its disposal to investigate terrorism crimes, I am here today to ask you to make permanent sections 201 and 202 of the USA PATRIOT Act. In addition, if section 223 were allowed to

expire, then individuals whose privacy might have been violated through the use of these tools would be denied an important avenue for redress.

II. Section 201

In the criminal law enforcement context, federal investigators have long been able to obtain court orders to intercept wire communications (voice communications over a phone) and oral communications (voice communications in person) to investigate numerous criminal offenses listed in the federal wiretap statute. The listed offenses include traditional crimes, including drug crimes, mail fraud, and passport fraud. Prior to the enactment of the USA PATRIOT Act, however, certain extremely serious crimes that terrorists are likely to commit, such as those involving chemical weapons, the killing of United States nationals abroad, the use of weapons of mass destruction, and the provision of material support to foreign terrorist organizations, were not among them. This prevented law enforcement authorities from using many forms of electronic surveillance to investigate these serious criminal offenses. As a result, law enforcement could obtain, under appropriate circumstances, a court order to intercept phone communications in a passport fraud investigation, but not a criminal investigation of terrorists using chemical weapons or murdering a United States national abroad.

Section 201 of the USA PATRIOT Act ended this anomaly in the law by amending the criminal wiretap statute. It added the following terrorism-related crimes to the list of wiretap predicates: 1) chemical weapons offenses; 2) murders and other acts of violence against United States national occurring outside the United States; 3) the use of weapons of mass destruction; 4) violent acts of terrorism transcending national borders; 5) financial transactions with countries that support terrorism; and 6) material support of terrorists and terrorist organizations. There

were also two other offenses that were subsequently added to this list which included bombings of places of public use, government facilities, public transportation systems, and infrastructure facilities, and financing of terrorism.

Section 201 of the USA PATRIOT Act preserved all of the pre-existing standards in the wiretap statute. For example, law enforcement still must apply for and receive a court order; establish probable cause to believe an individual is committing, has committed, or is about to commit a particular predicate offense; establish probable cause to believe that particular communications concerning that offense will be obtained through the wiretap; and establish that "normal investigative procedures" have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous.

Since the enactment of the USA PATRIOT Act, Justice Department investigators have utilized Section 201 to investigate, among other things, potential weapons of mass destruction offenses as well as the provision of material support to terrorists. In total, as of March 10, 2005, the Department utilized section 201 on four occasions. These four uses occurred in two separate investigations. One of those cases involved an Imperial Wizard of the White Knights of the Ku Klux Klan who attempted to purchase hand grenades for the purpose of bombing abortion clinics and was subsequently convicted of numerous explosives and firearms charges.

Section 201 is extremely valuable to the Justice Department's counterterrorism efforts because it enables criminal investigators to gather information using this crucial technique, subject to all of the requirements of the wiretap statute**,** when investigating terrorism-related crimes, and ensuring that these offenses are thoroughly investigated and effectively prosecuted**.** If wiretaps are an appropriate investigative tool to be utilized in cases involving bribery, gambling, and

obscenity, then surely investigators should be able to use them when investigating the use of weapons of mass destruction, chemical weapons offenses, and other terrorism-related offenses.

III. Section 202

Just as many traditional terrorism-related offenses were not listed as wiretap predicates before the passage of the USA PATRIOT Act, neither were many important cybercrime or cyberterrorism offenses, offenses concerning which law enforcement must remain vigilant and prepared in the 21st Century. Therefore, once again, while criminal investigators could obtain wiretap orders to monitor wire and oral communications to investigate gambling offenses or other crimes, but they could not use such techniques in appropriate cases involving certain serious computer crimes. Section 202 of the USA PATRIOT Act eliminated this anomaly by allowing law enforcement to use pre-existing wiretap authorities to investigate felony offenses under the Computer Fraud and Abuse Act, and brought the criminal code up to date with modern technology.

As with section 201, section 202 of the USA PATRIOT Act preserved all of the pre-existing standards in the wiretap statute, ensuring that law enforcement still must apply and receive a court order; establish probable cause to believe an individual is committing or about to commit the predicate offense; establish probable cause to believe that particular communications about the offense will be obtained through the wiretap; and establish that normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous.

As of March 10, 2005, the Justice Department had used section 202 of the USA PATRIOT Act on two occasions. These two uses occurred in a computer fraud investigation that eventually broadened to include drug trafficking. If section 202 were allowed to expire, then investigators would not be able to obtain wiretap orders to investigate many important cybercrime and cyberterrorism offenses, resulting in a criminal code that is dangerously out of date compared to modern technology.

IV. Section 223

Prior to the enactment of the USA PATRIOT Act, individuals were permitted only in limited circumstances to file a cause of action and collect money damages against the United States if government officials unlawfully disclosed sensitive information collected through the use of court-approved investigative tools. For example, while those engaging in illegal wiretapping or electronic surveillance were subject to civil liability, those improperly disclosing information obtained from lawful pen register orders or warrants for stored electronic mail generally could not be sued. Section 223 of the USA PATRIOT Act remedied this inequitable situation by creating an important mechanism for deterring the improper disclosure of sensitive information and providing redress for individuals whose privacy might be violated by such disclosures.

Under section 223, a person harmed by a willful violation of the criminal wiretap statute or improper use and disclosure of information contained in the Foreign Intelligence Surveillance Act**,** [FISA] may file a claim against the United States for at least $10,000 in damages, plus costs. The section also broadened the circumstances under which administrative discipline may be imposed upon a federal official who improperly handled sensitive information by requiring the agency to initiate a proceeding in order to determine the appropriate disciplinary action.

To date, no complaints have been filed against Department employees pursuant to section 223. This is a reflection of the professionalism of the Department's employees as well as their commitment to the rule of law. Although there have been no allegations of abuse[s] under this section, it is important that section 223 remain in effect as it provides an important disincentive to those would unlawfully disclose intercepted communications. Most everyone who has reviewed this provision agrees that it is a valuable tool that should certainly be renewed. In addition, section 223 clearly demonstrates the PATRIOT Act's concern, not just the security of the United States, but also for the civil liberties of its citizens.

V. Conclusion

Thank you once again for the opportunity to discuss sections 201, 202, and 223 of the USA PATRIOT Act. These provisions are critical to the Department's efforts to protect Americans from terrorism. From my experience as a prosecutor, I know firsthand how valuable wiretaps are to the investigation and prosecution of serious criminal offenses. There is no logical reason why these valuable tools should not be extended to allow law enforcement to protect our citizens from terrorism-related offenses as well. I am happy to answer any questions you might have.